

The Honorable Richard A. Jones

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

V.

ROMAN VALEREYVICH SELEZNEV,

Defendant.

NO. CR11-0070RAJ

**RESPONSE TO DEFENDANT'S
MOTION TO EXCLUDE "OTHER
ACTS" EVIDENCE**

NOTED: August 3, 2016

1. INTRODUCTION

The Second Superseding Indictment charges defendant with engaging in a scheme to defraud that included stealing credit card data from “hundreds of retail businesses . . . including but not limited” to 62 businesses identified in the indictment. Dkt. 90 at ¶ 17. The indictment alleges that defendant executed this scheme to defraud in this district by means of 11 specific wire transmissions involving local victims, such as Mad Pizza and Grand Central Baking.

Defendant moves to exclude evidence of intrusions other than the 11 wire transmissions charged as executions. Dkt. 365. Defendant mistakenly characterizes these intrusions as “separate and distinct criminal acts,” when they are in fact part of the single scheme to defraud with which defendant is charged. *Id.* at 1.

Defendant’s motion is contrary to black-letter law. It is well established that, in a prosecution alleging a scheme to defraud (such as a mail fraud or wire fraud prosecution), the government is entitled to present evidence of the entire scheme to defraud, and is not confined by the specific wirings or mailings charged as executions of the scheme. In this case, evidence of defendant’s hundreds of intrusions is direct evidence of the existence of a scheme to defraud, and is not “other acts” evidence subject to Rule 404(b) as defendant suggests. Accordingly, the motion should be denied.

II. BACKGROUND

A. The Scheme to Defraud

On October 8, 2014, the grand jury returned a Second Superseding Indictment (hereinafter “the indictment”) charging defendant with, *inter alia*, 11 counts of wire fraud in violation of 18 U.S.C. § 1343 and 2. The indictment sets forth the object of the scheme to defraud as follows:

The object of the scheme and artifice to defraud was to obtain, market, and sell stolen credit card numbers on underground websites for the purpose and with the intent that the stolen credit card numbers would then in turn be used for fraudulent transactions across the United States and in foreign countries, thereby defrauding the issuing banks and the merchants that accepted the cards for payment based on the false pretense that the users of the stolen credit card numbers were authorized users of those credit card numbers. By way of this series of criminal actions, the defendant intended to and did generate and receive millions of dollars in illicit profits, and caused millions of dollars in losses to banks and merchants.

See Second Superseding Indictment, Dkt. 90 at p. 2, ¶2.

The indictment alleges defendant, “and others known and unknown to the Grand Jury,” configured multiple “dump collection” servers including a server in McLean, Virginia to receive and compile the stolen credit card numbers that defendant hacked as part of a wide ranging scheme to target point of sale systems all over the world. *Id.* at p. 4, ¶ 8. In addition, the indictment alleges that defendant and his co-conspirators scanned

1 computers throughout the world for vulnerabilities that they could use to facilitate their
 2 fraud scheme. *Id.* ¶ 10.

3 The indictment plainly defines the scope of the scheme to defraud as including
 4 intrusions into hundreds of businesses. Specifically, the indictment alleges that, through
 5 the use of the techniques described above, defendant identified, hacked into, and stole
 6 data from “*hundreds of retail* businesses in the Western District of Washington and
 7 elsewhere *including, but not limited to . . .*” 62 business locations named in the
 8 indictment. *Id.* at p. 6, ¶ 16 (emphases added).

9 At trial, the evidence will show that the hundreds of attacks were part of a single
 10 scheme achieved using common methods and computer infrastructure. For example,
 11 Detective Dunn will testify the evidence he gathered with respect to these hundreds of
 12 victims showed: 1) all were infected with the same family of custom malware; 2) the
 13 majority used similar point of sale software; 3) most had been hacked via compromise of
 14 remote desktop access; and 4) most were engaged in a similar business operations
 15 (primarily restaurants, particularly pizza restaurants). The data from all attacks was then
 16 offered for sale on defendant’s websites.

17 **B. Execution of the Scheme to Defraud**

18 The wire fraud statute requires the government to prove that the scheme to defraud
 19 was executed by means of at least one interstate or foreign wire transmission in
 20 furtherance of the fraud. 18 U.S.C. § 1343. To establish venue, the indictment must
 21 charge that at least one of the wirings was “begun, continued or completed” in this
 22 district. *United States v. Pace*, 314 F.3d 344, 350 (9th Cir. 2002). Accordingly,
 23 Paragraph 32 of the Indictment alleges, as executions, 11 specific wirings in this district
 24 in furtherance of the fraud. These examples are just a small subset of the many (probably
 25 tens of thousands of) wirings that defendant used in the course of his scheme. The
 26 charged executions include transmissions to local businesses including several Mad Pizza
 27 locations, Grand Central Baking Company and Broadway Grill. Dkt. 90 ¶ 32.
 28

III. ARGUMENT

Defendant contends that evidence of intrusions other than the 11 listed executions constitutes “other acts” evidence that should be excluded under Rule 404(b). Rule 404(b) applies when the government seeks to introduce evidence of conduct *other than* that charged in the indictment. Here, however, the hundreds of intrusions at issue are part of the charged scheme, and are therefore admissible to prove that scheme. The evidence is thus not “other acts” evidence at all, and does not implicate Rule 404(b).

To sustain a conviction for wire fraud, the government must prove, *inter alia*, (1) the *existence* of a scheme to defraud; and (2) that fraud scheme was *executed* by means of interstate or foreign wire transmissions. Ninth Circuit Model Instruction 8.124. The flaw in defendant's motion is that it confuses these two elements and mistakenly assumes that the scope of the scheme to defraud is limited to the executions (wirings) listed in the indictment. This is not the law.

The Ninth Circuit and other courts have repeatedly held that, in proving the existence of a scheme to defraud, the government is entitled to present evidence of the entire scheme. The government is not limited (as defendant asserts here) to evidence of victims involved in the charged executions. *United States v. Montgomery*, 384 F.3d 1050, 1061-62 (9th Cir. 2004) (in prosecution alleging nineteen counts of mail fraud, government was properly allowed to present evidence of more than one thousand incidents of fraud); *United States v. Mundi*, 892 F.2d 817, 820 (9th Cir. 1989) (where wire fraud indictment referred to a single victim but described the scheme “in terms that indicated a far wider scope of operations,” government properly introduced evidence of other victims of the same scheme not referenced in the indictment); *see United States v. Dula*, 989 F.2d 772, 777 (5th Cir. 1993) (in wire fraud prosecution, evidence of fraud on victims not referenced in the indictment “was relevant to the existence of a scheme to defraud and therefore independently admissible as direct proof of the scheme charged”); *United States v. Roylance*, 609 F.2d 164, 167 (10th Cir. 1982) (in mail fraud prosecution, evidence of fraudulent transactions other than those specified in the indictment “did not

1 constitute excludable other crimes evidence, but proof highly probative of the existence
 2 of the very scheme” charged in the indictment); *United States v. Nelson*, 570 F.2d 258,
 3 262 (8th Cir. 1978) (rejecting argument that court should have excluded evidence of
 4 conduct occurring before the charged wirings; “evidence presented concerning the
 5 existence of a scheme . . . prior to the placing of the calls was appropriately introduced to
 6 prove one of the elements, *i.e.*, a scheme to defraud”).¹

7 As discussed above, the indictment alleges that the scheme to defraud includes
 8 hundreds of victims, “including but not limited to” the 67 victims referenced in Paragraph
 9 16 of the indictment. Here, while the execution section of the indictment (Paragraph 32)
 10 focuses on 11 specified wirings in this district, the indictment alleges a scheme that goes
 11 far beyond those wirings. The charged scheme includes hacking into point of sale
 12 systems, stealing credit cards, and trafficking in those stolen credit cards over the
 13 internet. The indictment alleges—and the evidence will show—that defendant used the
 14 same malicious software, the same servers, the same email accounts and the same
 15 websites to steal and sell credit card data from hundreds of victims. Therefore, all of
 16 these intrusions are part of a single inextricably intertwined scheme to defraud, and
 17 evidence of those intrusions is not evidence of “other acts” implicating Rule 404(b).

18 //

19 //

20 //

21

22

23

24

25

26 ¹ The same rule is applied in conspiracy cases, which generally follow the same principles as mail fraud
 27 and wire fraud cases. *United States v. Rizk*, 660 F.3d 1125, 1131 (9th Cir. 2011) (recognizing the “well
 28 established rule that the government in a conspiracy case may submit proof of the full conspiracy; it is not
 limited in its proof to the overt acts alleged in the indictment”); see *United States v. Stapleton*, 293 F.3d
 1111, 1117 (9th Cir. 2002) (noting that the law of conspiracy and schemes to defraud are generally
 “parallel” and that “similar evidentiary rules apply” to conspiracies and schemes to defraud).

1 **IV. CONCLUSION**

2 Under the authorities discussed above, the government is entitled to present
3 evidence of the full scope of the fraud to meet its burden of proving the existence of a
4 scheme to defraud. The motion should be denied.

5 DATE: July 29, 2016.

6
7 ANNETTE L. HAYES
8 Acting United States Attorney

LESLIE R. CALDWELL
Assistant Attorney General

9 /s/ Norman M. Barbosa
10 NORMAN M. BARBOSA
11 Assistant United States Attorney
12 Western District of Washington

/s/ Harold Chun
HAROLD CHUN
Trial Attorney
Computer Crime and Intellectual
Property Section

13
14 /s/ Seth Wilkinson
15 SETH WILKINSON
16 Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that on July 29th, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the attorney of record for Defendant.

s/ Jennifer J. Witt
JENNIFER J. WITT
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: 206-553-2520
Fax: 206-553-2502
E-mail: Jennifer.Witt@usdoj.gov